UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 05/05/2005

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/771,967	AKKAR ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20050121*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 21 January 2005. Claims 1-13 have been canceled. New Claims 14-33 have been added. Claims 14-33 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments with respect to claims 14-33 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

3. Claim 14 is objected to because of the following informalities: Claim 14 recites the limitation "in order to resist to an attack" in line 3 of the claim. It appears that this is intended to read, "in order to resist an attack". Appropriate correction is required.

4. Applicant is advised that should claims 23 and 24 be found allowable, claims 32 and 33 will be objected to under 37 CFR 1.75 as being substantial duplicates thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 14-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In reference to Claim 14, as written, the "step of determining" appears to include the steps of "outputting" and "comparing", recited following the step of "randomly selecting". However, it does not appear that the steps of outputting and comparing are actually perform any part of the step of determining. The step of "outputting as the resultant message", if included in any previously recited limitation, would, at best, appear to be a part of the step of "applying the second chain of operations... so as to obtain a resultant message". Further, the step of "comparing the resultant message to the result" appears to be entirely independent of the steps of determining and applying. These limitations make the claim unclear, and therefore indefinite. Further, it is not clear whether the limitation "a last operation of the first chain of operations", recited in the step of outputting, refers to the first chain of operations applied to the message by the first entity or to the part of the operations that are randomly selected as part of the step of determining.

Claims 15-19 recite the limitation "the at least a part of the first chain of operations which can be performed in a complemented state". There is insufficient antecedent basis for this limitation in the claims.

Claim 20 recites the limitation "each of a series of several parts" in line 5; however, line 6 refers to "either such part", which appears to refer to only two such parts. This appears to be inconsistent with the number of "each of a series of several parts", as that limitation can refer two more than two parts. This inconsistency renders the claim indefinite.

Similarly, Claim 21 recites the limitation "each of a series of operations" in line 5 and the limitation "either such operation" in lines 6-7. The numbers of "each of a series of several" and "either" appear to be inconsistent, which renders the claim indefinite. Further, it is noted that the limitation "adjacent or not" in line 6 does not further limit the claim.

Claims 22, 23, 31, and 32 recite the limitation "the at least a part of the first chain of operations". It is unclear whether this refers to the "at least a part of the first chain of operations" or to the "at least a part of the first chain of operations performed in a complemented state" of Claim 14. Claims 23 and 32 also recite the limitation "the chain of operations"; it is not clear whether this refers to the first or second chain of operations of Claim 14, or one of the "at least part of the first chain of operations" referred to above. These limitations render the claims indefinite. Additionally, the claims recite the limitation "deciding the step of outputting". This limitation is generally unclear, as it is not clear what specifically regarding the step of outputting is decided.

Claims 24 and 33 recite the limitations "the step of randomly determining and applying the similar chain of operations", "the computing of a parameter", and "the decision to perform". There is insufficient antecedent basis for these limitations in the claims. Further, the claims refer to an operation of the first chain of operations being performed. It is unclear whether this is intended to refer to the first chain of operations being performed when applied within the first entity, or to the at least a part of the operations that can be selected in the step of determining the second chain of operations to be applied within the second entity. These limitations render the claims indefinite.

Claim 25 recites the limitation "the step of randomly determining". There is insufficient antecedent basis for this limitation in the claims.

Claim 26 recites the limitations "the step of randomly selecting and applying" and "the decision to perform". There is insufficient antecedent basis for these limitations in the claims. Further, the claim refers to an operation of the first chain of operations being performed. It is unclear whether this is intended to refer to the first chain of operations being performed when applied within the first entity, or to the at least a part of the operations that can be selected in the step of determining the second chain of operations to be applied within the second entity. These limitations render the claim indefinite.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 14-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Kocher et al, US Patent 6278783, and Chow et al, US Patent 6594761.

In reference to Claim 14, Applicant admits as prior art a method including applying a message to first and second electronic entities, applying a first chain of operations to the message within the first entity to obtain a result, applying a second chain of operations to the message within the second entity to obtain a resultant message, and comparing the resultant message to the result (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly selecting to perform operations of the first chain in either a normal or a complemented state.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify the prior art method by including a random determination of which operations in the chain to carry out, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9). However, Kocher does not explicitly disclose performing operations in either a normal state or a complemented state.

Chow discloses a tamper-proofing encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the method, described in Applicant's admitted prior art and modified by Kocher, by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 20 and 21, Chow further discloses that a decision whether to perform an operation or its complement is made for each operation (column 18, line 65-column 19, line 13).

In reference to Claims 22 and 31, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and a counter is updated (column 9, lines 25-27).

In reference to Claims 23 and 32, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and intermediate responses are transmitted (see column 2, lines 17-19).

In reference to Claims 24, 26, and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30).

In reference to Claim 25, Kocher further discloses two chains of operations (column 6, lines 28-38 and 64-67).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Harrison, US Patent 5870468, discloses a method for protecting files that includes storing a key in a scrambled form, that can include taking the complement of the key.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ZAD
zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER